



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/810,025

03/26/2004

John J. Apostolopoulos

200401716-1

8407

22879 7590 10/11/2007

HEWLETT PACKARD COMPANY  
P O BOX 272400, 3404 E. HARMONY ROAD  
INTELLECTUAL PROPERTY ADMINISTRATION  
FORT COLLINS, CO 80527-2400

EXAMINER

HOANG, DANIEL L

ART UNIT

PAPER NUMBER

2136

MAIL DATE

DELIVERY MODE

10/11/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/810,025

Applicant(s)

APOSTOLOPOULOS ET AL.

Examiner

Daniel L. Hoang

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 26 March 2004.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-34 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-34 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 11/10/05.
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application
- ☐ Other: \_\_\_\_\_

## DETAILED ACTION

### CLAIMS PRESENTED

Claims 1-34 are presented.

### CLAIM REJECTIONS

#### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 1-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chang et al., US Patent No. 6,963,972, and further in view of Recommendation of Block Cipher Modes of Operation – Methods and Techniques, hereinafter NIST.**

**As per claim 1, 12, 24:**

Chang teaches:

A method for generating transcodable encrypted content that comprises independently processable components, said method comprising:

accessing transcodable content that comprises independently processable components to be encrypted;  
and

*[see col. 3, lines 51-62]*

encrypting at least one of said independently processable components to provide independently processable components which are independently decryptable,

*[see col. 3, lines 51-62 and col. 4, lines 19-29]*

said encrypting performed using an encryption scheme [that utilizes non-repeating identifiers] that uniquely correspond to said independently processable components, wherein said transcodable encrypted content is transcodable without requiring knowledge of said encryption scheme.

*[see col. 10, lines 24-41]*

*Chang is not explicit in teaching that the encryption scheme utilizes non-repeating identifiers.*

NIST teaches the Counter block cipher mode of operation (see page 15, section 6.5). The counter mode is an encryption/decryption scheme that utilizes non-repeating identifiers/counters. It would have been obvious to one of ordinary skill in the art to utilize a counter mode as the encryption algorithm used in the Chang reference. One would have been motivated to do so in order to optimize operations on a multi-processor machine where blocks can be encrypted in parallel.

**As per claim 2, 13, 25, Chang teaches:**

The method as recited in claim 1 wherein said independently processable components comprise components that are independently decodable and independently authenticatable.

*[see col. 3, lines 51-62 and col. 4, lines 19-29]*

**As per claim 3, 14, 26, NIST teaches:**

The method as recited in claim 1 wherein said encryption scheme comprises applying block ciphers in stream cipher mode.

*[see page 15, section 6.5]*

**As per claim 4, 15, 27, NIST teaches:**

The method as recited in claim 1 wherein said encryption scheme comprises counter (CTR) mode stream cipher encryption.

*[see page 15, section 6.5]*

**As per claim 5, 16, 28, NIST teaches:**

The method as recited in claim 1 wherein said encryption scheme comprises encrypting a counter to generate a keystream which is logically combined with plaintext to generate ciphertext.

*[see page 15, section 6.5]*

**As per claim 6, 17, 29, NIST teaches:**

The method as recited in claim 1 wherein said encryption scheme utilizes non-repeating identifiers which are non-repeating counter values.

*[see page 15, section 6.5]*

**As per claim 7, 18, 30, NIST teaches:**

The method as recited in claim 1 wherein said encryption scheme comprises performing several encryptions in parallel.

*[see page 15, section 6.5]*

**As per claim 8, 19, 31, Chang teaches:**

The method as recited in claim 1 wherein differentiating metadata that corresponds to said independently processable components is used as an input to said encryption.

*[see col. 9, lines 24-45]*

**As per claim 9, 21, 32, Chang teaches:**

The method as recited in claim 1 wherein said transcodable encrypted content has information associated with it to direct transcoding.

*[see col. 10, lines 42-65]*

**As per claim 10, 22, 33, Chang teaches:**

The method as recited in claim 1 said transcodable encrypted content comprises respective components that have respective encryption keys, wherein said respective encryption keys are related to a root encryption key.

*[see col. 10, lines 24-41]*

**As per claim 11, 23, 34, NIST teaches:**

The method as recited in claim 1 wherein said encryption scheme is selected from the group consisting of a block cipher used in output feedback (OFB) mode, RC4, SEAL, and WAKE.

*[see page 13, section 6.4]*

**As per claim 20, Chang teaches:**

The method as recited in claim 12 wherein said transcoding produces transcodable encrypted content that is smaller in size than the transcodable encrypted content that is accessed.

*[see col. 9, lines 1-23]*

**CONCLUSION**

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

**POINTS OF CONTACT**

- \*. Any response to this Office Action should be **faxed to (571) 273-8300 or mailed to:**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**Hand-delivered responses** should be brought to

Customer Service Window  
Randolph Building  
401 Dulaney Street

Art Unit: 2136

Alexandria, VA 22314

\*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

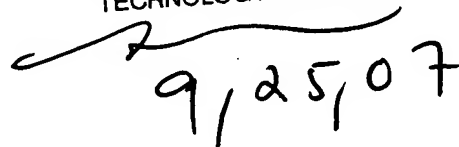
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

*Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).*



Daniel L. Hoang  
9/25/07

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100



9,25,07